SECS1024 - Laboratoire 5 - protection HTTPS

Ce laboratoire est not´e - 15 points - 10% de la note finale

a` rendre pour mardi 18 f´evrier

Objectif : prot´eger une application web avec le chiffrement de la couche application en HTTPS.

Mise en place du laboratoire : utilisez pour ce laboratoire une VM Kali et une VM wordpress connect´ees en r´eseau interne VirtualBox. **Indiquez ci-dessous les adresses IP de ces deux VMs (0,5 point) :**

Vous devez illustrer toutes vos r´eponses par des captures ´ecran pour obtenir tous les points.

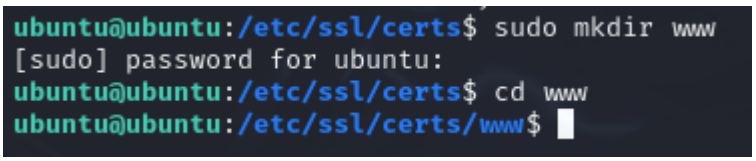
```
┌──(kali㉿kali2024blue)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4d:5d:52 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.5/24 brd 192.168.2.255 scope global dynamic noprefixroute eth0
       valid_lft 445sec preferred_lft 445sec
    inet6 fe80::a00:27ff:fe4d:5d52/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

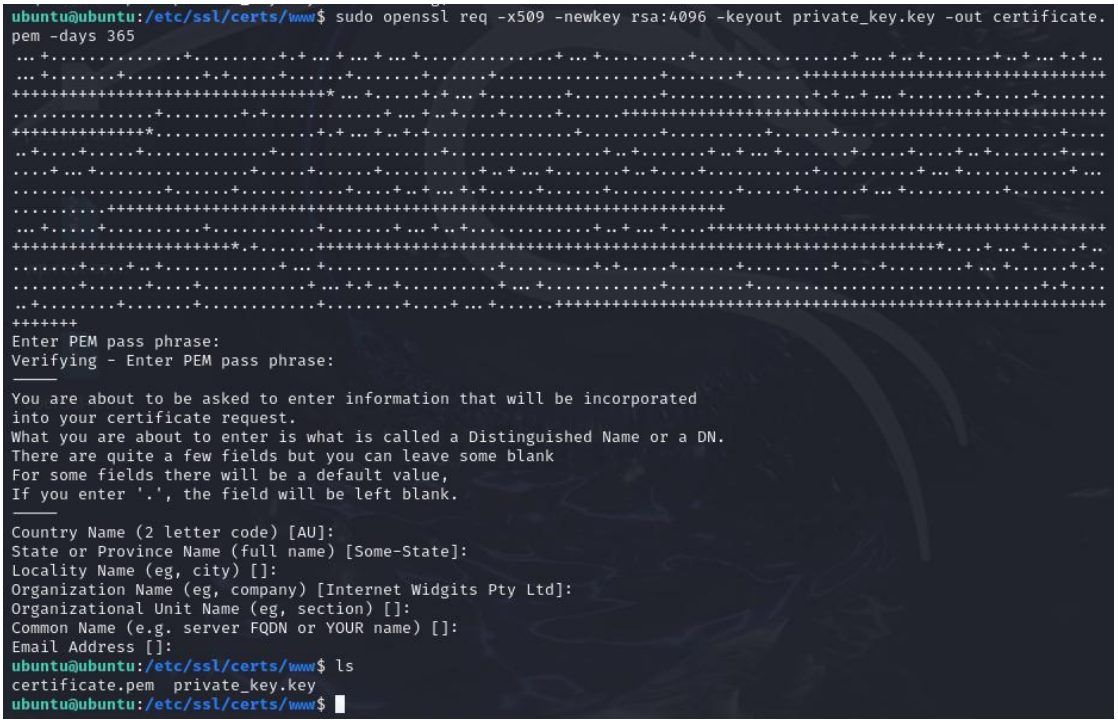
```
ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0b:13:0d brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.6/24 metric 100 brd 192.168.2.255 scope global dynamic enp0s3
       valid_lft 562sec preferred_lft 562sec
    inet6 fe80::a00:27ff:fe0b:130d/64 scope link
       valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$
```

1 Certificat X509 (6 points)

Dans un premier temps, vous allez cr´eer sur la VM Wordpress un certificat au format X509. Ce certificat va contenir des informations sur votre application wordpress et surtout la cl´e publique RSA qui sera utilis´ee pour chiffrer la communication entre le client et le serveur et permettre ainsi de passer en HTTPS.

1) Sur Kali, connectez-vous en ssh sur la VM wordpress. Dans le dossier /etc/ssl/certs de la VM wordpress, cr´eez un dossier www et placez-vous dans ce dossier. Quelle commande openssl permet de cr´eer un certificat X509 auto-sign´e contenant une cl´e publique RSA 4096 bits (aide : man openssl req) ? Utilisez cette commande dans le dossier /etc/ssl/certs/www/. Faites des captures ´ecran de la commande et de la liste des fichiers obtenus. (5 points)





2) Quelle commande permet d’afficher en texte le contenu du certificat ? (1 point)

```
ubuntu@ubuntu:/etc/ssl/certs/www$ openssl x509 -inform PEM -in certificate.pem -noout -text
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number:
            63:95:39:6a:f4:66:fd:65:2c:6a:de:3c:19:e9:d0:51:95:d9:36:aa
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
        Validity
            Not Before: Feb 18 13:56:09 2025 GMT
            Not After : Feb 18 13:56:09 2026 GMT
        Subject: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:ba:c8:16:45:53:a2:5c:66:39:2d:5a:e9:c5:59:
                    e0:45:fd:c6:b0:4b:a3:a4:94:13:30:3c:47:9e:ff:
                    97:1d:84:aa:31:5b:df:bf:4d:73:aa:60:bf:2d:d8:
                    cb:f2:09:1d:75:02:63:2f:e0:3d:b0:9c:e2:0e:83:
                    da:06:0d:63:61:b9:1b:5b:f8:e2:10:fa:a7:ab:bc:
                    ed:7a:aa:9c:80:39:2d:a0:7f:27:34:ca:7b:c9:3a:
                    ff:2b:9a:ca:3c:53:7c:b6:66:c3:05:a2:9c:7b:58:
                    60:3e:c2:6f:5c:ca:fe:0c:b2:06:41:01:a6:69:a1:
                    c4:dc:6a:8f:c0:ec:ec:a4:81:e7:de:01:6a:70:75:
                    6c:d8:aa:2d:ef:8a:78:db:83:5a:03:9f:1f:82:0a:
                    e8:5a:6d:50:dd:64:e3:c6:82:62:f6:df:eb:92:a3:
                    0a:20:79:2b:43:25:df:e0:0a:ac:b7:e4:4a:1b:6b:
                    55:d5:74:9b:2a:52:51:7c:01:66:90:2d:94:fc:fe:
                    22:2d:b4:5f:75:22:c7:df:b4:99:e1:0f:79:84:fc:
                    f2:bc:a8:8b:45:92:88:c8:86:74:a6:ce:11:87:29:
                    30:c0:67:ab:a0:b5:1c:4a:05:36:f2:a2:c0:8a:b9:
                    60:07:df:e8:76:d0:71:83:54:fb:2b:14:25:9c:6d:
                    a2:16:2e:0c:1e:85:56:9f:a5:ea:f2:c9:6f:9e:32:
                    48:ec:e8:89:a1:e8:fd:44:53:7c:0c:b0:b0:b9:c5:
                    f6:ca:70:d1:45:bf:a3:7f:c4:ab:fa:6d:b1:c4:7d:
                    87:0e:b2:fc:2b:98:82:1c:f7:c8:59:1f:bc:10:3c:
                    b8:86:8e:87:40:4d:37:ad:f7:47:e0:46:a5:9e:e4:
                    db:53:70:5f:39:78:7c:ad:09:8e:85:70:a4:1e:95:
                    c6:4e:74:4b:c9:70:f7:5b:f5:5d:0e:25:49:86:15:
                    66:c1:6f:99:94:19:99:c5:b4:83:ed:c6:ac:71:d5:
                    57:c6:61:51:28:20:73:71:0e:96:78:dc:6d:cf:ac:
                    38:bc:d3:31:b0:4a:bd:74:75:e1:15:43:b6:98:8a:
                    db:7d:14:52:28:18:6a:9d:e0:47:e4:a9:f0:7b:41:
                    c4:28:e0:8b:52:fd:0b:19:be:7b:19:dd:74:c9:ff:
                    47:c6:b0:48:6a:d4:6e:cd:9c:69:65:1e:28:ee:af:
                    70:20:32:a5:86:ef:55:07:55:4e:6d:3c:f6:52:86:
                    42:ef:4c:84:3c:44:a7:64:a4:86:ac:35:bf:75:d4:
                    2d:af:8c:30:d7:3b:5d:cb:a0:30:5d:e7:14:0d:0f:
                    f8:04:52:68:38:88:35:8a:64:47:20:7d:93:70:1a:
                    26:62:fb
                Exponent: 65537 (0×10001)
```

```
                26:62:fb
            Exponent: 65537 (0×10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                E9:75:9D:09:2C:3D:2D:CE:23:C4:15:EE:D9:C9:43:EF:88:1C:7D:99
            X509v3 Authority Key Identifier:
                E9:75:9D:09:2C:3D:2D:CE:23:C4:15:EE:D9:C9:43:EF:88:1C:7D:99
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        67:ce:ab:c0:38:79:67:b1:dc:13:94:9d:fe:a0:f1:7d:9e:df:
        c9:89:74:23:4d:2c:0e:27:64:ff:ad:da:f2:09:24:7e:53:be:
        a1:36:8f:03:2f:21:c4:b5:ca:54:71:8e:5b:90:fa:b5:f2:a8:
        ac:5f:67:2a:b3:5b:fa:ab:8e:a3:7f:8a:0b:a1:66:8d:79:a9:
        64:f0:25:4f:e7:ad:15:3d:34:41:80:5a:f5:2e:25:df:e4:48:
        89:f2:c5:25:95:9f:4e:b1:91:ef:d8:aa:c7:be:58:db:7c:54:
        e2:88:dc:cd:6e:fe:63:8b:1f:98:bf:98:2e:9e:cd:8a:71:b4:
        2a:61:79:f7:c0:14:ca:96:4e:86:41:60:1f:07:3a:ca:52:8a:
        5a:c4:17:d4:24:bd:39:32:6d:dd:8a:d6:b4:e4:dc:93:68:41:
        8f:6c:e2:c4:01:4f:d7:b5:9f:c9:b9:fa:37:00:25:7b:7f:ee:
        89:65:ac:c0:00:97:aa:73:14:ea:a5:f2:2b:6b:a6:05:4b:16:
        bf:24:c1:ac:a0:6c:e9:e7:5f:8d:09:89:5b:4f:9b:ed:fb:a9:
        81:02:c0:69:2d:c9:f2:4f:85:f2:af:d7:b2:47:27:09:cf:d4:
        f4:fa:bf:1c:0b:75:b8:3b:c0:da:a6:27:5e:48:31:51:4d:c1:
        d8:c3:af:d2:bd:11:6e:e9:65:56:2a:3d:44:d3:26:4e:52:4e:
        0f:4a:00:82:c0:b6:2c:dd:4c:5b:d7:ad:06:66:19:c6:4b:0b:
        be:1f:c2:5c:76:88:3d:25:9f:0e:52:bc:ef:23:49:15:b2:fe:
        9b:54:0b:02:f2:b6:36:7e:52:e9:38:4d:0f:23:fb:20:a8:96:
        49:17:0b:dd:af:16:1c:5f:87:1d:85:32:ac:1d:13:a4:48:8f:
        64:a0:d0:1c:51:74:76:1b:e8:3c:1c:63:a5:29:2d:60:67:1e:
        d2:4a:af:dd:a5:97:6c:ff:82:74:c3:91:d2:bb:6c:37:a3:09:
        07:06:e5:9e:b7:34:63:7b:49:62:b0:92:9a:ca:e6:b4:c3:04:
        5b:f5:40:97:d5:4f:b2:fc:a7:6f:f1:f4:aa:6d:e5:1f:2b:fd:
        89:0b:c1:3d:1a:08:0a:ee:6e:32:15:2c:0b:7e:ae:b8:d2:46:
        ee:5e:38:e4:91:94:e5:2c:92:6c:c7:8d:ad:8c:9c:b8:96:cd:
        26:fd:ee:5c:3b:4a:9b:41:da:ed:e8:97:97:4c:02:44:a8:11:
        99:3f:03:ef:39:a0:d6:a2:02:eb:59:d8:d3:42:80:35:03:e9:
        a7:8c:2c:f9:e6:b8:71:3e:74:88:54:93:8f:ed:46:e5:66:28:
        a3:61:65:cf:77:b3:42:02
```

2 HTTPS (8,5 points)

1) Quelle commande permet d'activer le module ssl d'apache2 sur la VM wordpress ? (1 point)

```
ubuntu@ubuntu:/etc/ssl/certs/www$ sudo a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
ubuntu@ubuntu:/etc/ssl/certs/www$ sudo systemctl restart apache2
ubuntu@ubuntu:/etc/ssl/certs/www$
```

2) Configuration du site en HTTPS. Pour activer le mode HTTPS de votre site, il faut modifier le fichier de configuration de votre site qui se trouve dans le dossier /etc/apache2/sites-available/. Editez ce fichier. Dupliquez tout le contenu de la structure :

<Virtualhost *:80> ... </Virtualhost>

dans le mˆeme fichier (en dessous de la premi`ere). Dans la structure dupliqu´ee, modifiez :80 par :443 pour indiquer au serveur que vous ajoutez un nouvel hoˆte virtuel (s´ecuris´e) sur le port 443

du serveur. puis ajoutez dans la structure dupliqu´ee les lignes suivantes : (modifiez les noms de fichiers avec ceux que vous avez cr´e´es dans la partie 1)

SSLEngine on
SSLCertificateFile /etc/ssl/certs/www/fichier-du-certficat
SSLCertificateKeyFile /etc/ssl/certs/www/fichier-de-la-cle-privee

D´ecrivez la fonction de chacune de ces 3 lignes. (1,5 point - 0,5 par ligne d´ecrite)

```
 GNU nano 7.2                                                wordpress
<VirtualHost *:80>
    DocumentRoot /srv/www/wordpress
    <Directory /srv/www/wordpress>
        Options FollowSymLinks
        AllowOverride Limit Options FileInfo
        DirectoryIndex index.php
        Require all granted
    </Directory>
    <Directory /srv/www/wordpress/wp-content>
        Options FollowSymLinks
        Require all granted
    </Directory>
</VirtualHost>
<VirtualHost *:443>
    DocumentRoot /srv/www/wordpress
    <Directory /srv/www/wordpress>
        Options FollowSymLinks
        AllowOverride Limit Options FileInfo
        DirectoryIndex index.php
        Require all granted
    </Directory>
    <Directory /srv/www/wordpress/wp-content>
        Options FollowSymLinks
        Require all granted
    </Directory>
SSLEngine on
SSLCertificateFile /etc/ssl/certs/www/certificate.pem
SSLCertificateKeyFile /etc/ssl/certs/www/private_key.key
</VirtualHost>
```

La première ligne active le module SSL pour le serveur web, cela permet au serveur d'accepter des connexions avec https.

La deuxième ligne spécifie le chemin du certificat pour établir une session sécurise avec le serveur.

La troisième ligne spécifie le chemin de la clé associe au certificat.

3) Quelle commande permet d'activer le nouveau fichier de configuration ? Affichez les ports ouverts de la VM wordpress et faites une capture ´ecran : (2 points)

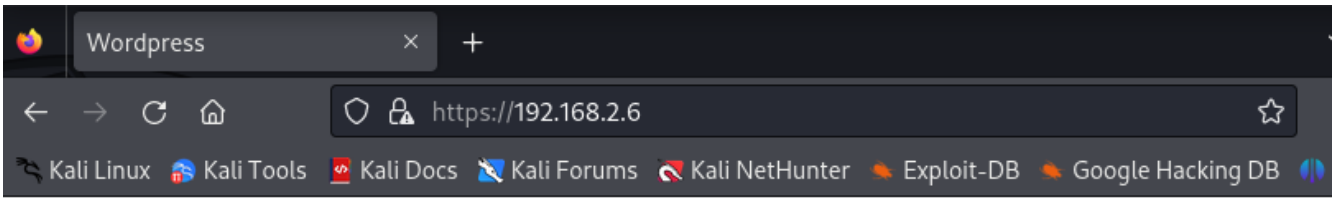
```
ubuntu@ubuntu:/etc/apache2/sites-available$ sudo a2ensite wordpress.conf
Site wordpress already enabled
ubuntu@ubuntu:/etc/apache2/sites-available$ sudo systemctl restart apache2
🔐 Enter passphrase for SSL/TLS keys for 127.0.1.1:443 (RSA): (press TAB for no echo)
Broadcast message from root@ubuntu (Tue 2025-02-18 14:18:10 UTC):

Password entry required for 'Enter passphrase for SSL/TLS keys for 127.0.1.1:443 (RSA):' (PID 1601).
Please enter password with the systemd-tty-ask-password-agent tool.

......
ubuntu@ubuntu:/etc/apache2/sites-available$
```

```
ubuntu@ubuntu:/etc/apache2/sites-available$ sudo ss -tuln
Netid     State      Recv-Q     Send-Q              Local Address:Port            Peer Address:Port     Process
udp       UNCONN     0          0                      127.0.0.54:53                 0.0.0.0:*
udp       UNCONN     0          0                   127.0.0.53%lo:53                 0.0.0.0:*
udp       UNCONN     0          0                192.168.2.6%enp0s3:68               0.0.0.0:*
tcp       LISTEN     0          151                    127.0.0.1:3306                 0.0.0.0:*
tcp       LISTEN     0          4096                127.0.0.53%lo:53                  0.0.0.0:*
tcp       LISTEN     0          70                     127.0.0.1:33060                0.0.0.0:*
tcp       LISTEN     0          4096                  127.0.0.54:53                   0.0.0.0:*
tcp       LISTEN     0          511                          *:80                         *:*
tcp       LISTEN     0          4096                         *:22                         *:*
tcp       LISTEN     0          511                          *:443                        *:*
```

4) D´emontrez, a` l'aide de captures ´ecran que la s´ecurit´e HTTPS de votre site wordpress est bien activ´ee (2 points)



5) Que faudrait-il faire pour que la s´ecurit´e HTTPS de votre site soit install´ee de mani`ere totalement s´ecuris´ee ? Argumentez votre r´eponse. (2 points) Fin du laboratoire. Il faudrait Mettre en place la redirection des requêtes http vers https pour que les utilisateur accèdent toujours à la version sécurisé du site.